The Honorable Brian A. Tsuchida

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. RIBEIRO TRELHA GUSTAVO, a/k/a Matos Fontinele, Defendant.	NO. MJ17-213 COMPLAINT for VIOLATION Title 18, United States Code, Sections 1029(a)(4) and 2

BEFORE the Honorable Brian A. Tsuchida, United States Magistrate Judge, United States Courthouse, Seattle, Washington.

The undersigned complainant being duly sworn states:

COUNT 1
(Access Device Fraud – Possession of Device-Making Equipment)

On or about April 27, 2017, in King County, within the Western District of Washington, the defendant, RIBEIRO TRELHA GUSTAVO, did knowingly and with intent to defraud, possess, produce, traffic in, and have custody and control of device-making equipment, specifically, card-encoding devices (also known as a "skimming devices"), which conduct affected interstate and foreign commerce through unauthorized

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

use of accounts at JP MorganChase, a financial institution with headquarters outside Washington State.

All in violation of Title 18, United States Code, Sections 1029(a)(4) and 2.

And the complainant states that this Complaint is based on the following information:

I, Michael P Germain, being first duly sworn on oath, depose and say:

I. BACKGROUND

1. I am a Special Agent with the United States Secret Service (USSS) and have been since March 3, 1987. I am currently assigned to the Seattle Field Office. I am a graduate of the Federal Law Enforcement Training Center located in Glynco, Georgia, and the United States Secret Service Special Agent Training Program located in Beltsville, Maryland. I have a Bachelor of Science Degree from Pennsylvania State University. As part of my training with the Secret Service, I have received instruction on the investigation of financial crimes, including credit/debit card fraud, mail and wire fraud, access device fraud and identity theft. I have also completed specialized training in the investigation of electronic crimes involving the use of computers and other electronic devices. In the course of my law enforcement career, I have investigated crimes ranging from the production and passing of counterfeit currency, identity theft, access device fraud, bank fraud and threats made against the President and Vice President of the United States. As part of my duties, I supervise the Seattle Electronic Crimes Task Force, which investigates crimes that use electronic devices to record, capture, produce, intrude, ex-filtrate, and transmit electronic data in furtherance of crimes.

2. This Affidavit is made in support of a complaint for the arrest of RIBEIRO TRELHA GUSTAVO, for violations of Title 18, United States Code,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Section 1029(a) (Access Device Fraud). The information contained in this Affidavit is based on my own personal knowledge and information provided to me during my participation in this investigation, including information provided by other law enforcement officers and witnesses. This Affidavit is submitted solely for the purpose of establishing probable cause for the charge alleged in this Complaint and does not purport to set forth all of my knowledge of, or investigation into, this case.

II. INVESTIGATION

3. This case involves a skimming operation in which card data is stolen from credit/debit cards and encoded onto various plastic cards with magnetic stripes. These same cards are then used, at least in part, to withdraw funds from unsuspecting victim account holders using Automated Teller Machines ("ATMs") in a "cash out" scheme.

A. Background: Skimming and Skimming Devices

4. Credit/debit card "skimming" is the theft of credit/debit card information used in an otherwise legitimate transaction. Among other techniques, suspects often use a small device (the "skimmer" or "skimming device") to steal data, or track data, of an unsuspecting victim's bank card. Skimming devices are often capable of holding data pertaining to hundreds or even thousands of bank cards. Most skimming devices have an integrated USB port, which allows data captured on the skimmer to be downloaded onto a laptop or desktop computer.

5. Suspects will typically connect the skimming devices to a computer, and then download the victim bank account data. Suspects will then transfer or "re-code" victim card data onto blank credit/debit card stock, also known as white plastic. Suspects have also been known to re-code stolen card data onto store gift cards. Any credit card sized plastic card with a magnetic stripe on the back of the card may be used to re-code victim card data and access funds in the victim's account. Given the nature of the activity, skimming necessarily requires use of a computer and other digital devices,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

including cameras, encoding equipment, such as credit card reader/writers, and USB devices.

6. Once this process is complete, suspects use the newly made cards to access victim bank account information at any available ATM machine or through point of sale purchases. Typically, suspects will withdraw cash and also purchase consumer goods and merchandise within a short period of time from the date that the debit card account was "skimmed." In some instances, however, suspects will wait several months before utilizing the stolen data. In either case, however, suspects will typically conduct numerous fraudulent transactions in a short time frame in order to maximize the use of the stolen data before the compromised bank or banks recognize the breach and begin shutting down the compromised accounts.

B. Evidence of Criminal Activity

7. This investigation originated on April 27, 2017, when, at approximately 5:34 p.m., Seattle Police Department was contacted by witness Chase Bank investigator Brandon Maylee regarding fraudulent activity at a bank ATM. Maylee reported that for the past three days, a white male suspect approached the stand-alone ATM located at 85 Pike St. and installed and then later removed a fraudulent bank card skimming device along with an electronic camera capable of capturing the customer/victims bank card and their Personal Identification Number (PIN) without the customer/victim realizing it. This conduct was observed through the camera on the ATM.

8. At approximately 8:00 p.m. the same evening, Maylee notified Seattle Police that he was currently watching real-time video using a camera located within the 85 Pike Street Chase Bank ATM. He advised that the same white male suspect who had previously been seen installing and removing the skimming device was currently at the ATM machine. He described the suspect as

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

being approximately 37 years old, 5'11" tall, 240-250 lbs, clean shaven, with short hair, and wearing a black leather jacket with red & black stripes on the sleeves and blue jeans.

9. SPD Officers Pirak and Belfiore arrived in the area and observed the individual later identified as GUSTAVO, who was wearing the described clothing, standing on the corner of 1st Avenue and Pike Street within 100 feet of the ATM machine. The officers stopped GUSTAVO and requested dispatch to have Maylee respond to their location. The officers were advised that Maylee was located out of state, but could make a positive identification if they walked the suspect over to the camera located within the ATM. The officers did so and Maylee positively identified GUSTAVO as the same person he had previously observed placing and removing the "skimmer device."

10. GUSTAVO was detained as Maylee described to officers the type of skimming device that was attached to the ATM machine. Officer Belfiore inspected the front of the ATM and was able with little effort to remove an improvised "skimming device" from the front of the ATM, on top of the ATM's original card reader. In addition to the "skimming device," Officer Belfiore removed an improvised camera attached to the ATM card slot in order to read the PIN number while the customer was inputting their PIN.

11. The SPD officers placed GUSTAVO under arrest for investigation of fraud. In a search incident to the arrest, officers recovered from GUSTAVO's person: one Extended Stay Hotel Room Access Card, ten suspected fraudulent cards (including nine credit cards and one Starbucks card), and a Brazilian identification card bearing GUSTAVO's picture and the name Matos Fontinele.

12. On April 28, 2017, Senior Special Agent (SSA) John Wurster and I responded to the Seattle Police Department East Precinct, where we were briefed on their investigation of GUSTAVO.

13. Seattle Police provided SSA Wurster the ten cards that were recovered from GUSTAVO's person at the time of his arrest. Using a magnetic stripe reader, SSA

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Wurster was able to confirm that seven of the bank cards embossed with the name of Fontinele and an embossed bank card number were found to have card numbers encoded on the magnetic stripe that were different from the embossed number on the bank card. Additionally, when the magnetic stripe on the Starbucks card was read by SSA Wurster, the number was identified as a MasterCard number. These mismatches between the information on the magnetic stripe and the outward appearance of the card are consistent with typical fraudulent identity theft conduct of utilizing a "skimming device" to capture a victim's credit card number and then using a Credit Card Eraser/Writer to apply this same number to any magnetic stripe on the back of a fraudulent credit card.

14. Also on April 28, 2017, I contacted Homeland Security Investigation (HSI) Special Agent Robert Patterson and provided him with the suspect's personal information obtained from his Brazilian driver's license bearing the name Fontinele. SA Patterson told me that there was no record for Fontinele in the HSI database. HSI maintains records of all individuals from foreign countries that enter the United States. There was no record of him entering the country.

15. Later that same date, Seattle Police detectives located the Extended Stay Hotel, in Bellevue, Washington, where GUSTAVO was currently staying. A search warrant was obtained and served on the hotel room. The following items were found in GUSTAVO's room:

One carry-on suitcase containing:

- Brazil Passport for GUSTAVO, Ribeiro Trelha
- Florida State Temporary Identification Card in the name GUSTAVO
- 3 Hard Drives
- 1 SD Card
- 2 Bank of America cards in the name GUSTAVO

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

One Federal Express Box addressed to Matos Fontinele containing:

- 3 modified ATM cameras
- 1 ATM Skimmer
- 1 Credit Card Reader/Writer

Recovered in the open area of the hotel room:

- Numerous blank credit cards
- Numerous gift cards with apparent PIN numbers listed on stickers
- Lenovo Computer Laptop
- Additional tools consistent with improvising and attaching devices to ATM's and building additional devices i.e., super glue, scissors, double stick tape.

16. On May 1, 2017, I again contacted SA Patterson and provided him with a photo of the passport found at the Extended Stay Hotel on April 28, 2017. SA Patterson stated that the individual on the passport was Ribeiro Trelha GUSTAVO of Brazil. He is a citizen of Brazil, and had overstayed his visa that expired in January 2016, after entering the United States in 2015.

17. Based upon the information provided by SA Patterson, I believe the Fontinele identification card found on GUSTAVO's person is fraudulent and the name of Matos Fontinele is an alias used by GUSTAVO.

III. CONCLUSION

18. Based on the above facts, I respectfully submit that there is probable cause to believe that RIBEIRO TRELHA GUSTAVO did knowingly and intentionally commit the offense of access device fraud – possession of device-making equipment, in violation of Title 18, United States Code, Sections 1029(a)(4) and 2.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

19. I declare under penalty of perjury that the above facts are true and correct to the best of my knowledge, information and belief.

Michael P. Germain, Complainant
Special Agent, United Stated Secret Service

Based on the Complaint and Affidavit sworn to before me, and subscribed in my presence, the Court hereby finds that there is probable cause to believe the Defendant committed the offense set forth in the Complaint.

Dated this 24th day of May, 2017.

HON. BRIAN A. TSUCHIDA
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970